REMARKS

In the Office Action dated August 11, 2004, claims 1-23 were rejected under the judicially created doctrine of obviousness-type double patenting over claims of U.S. Patent No. 6,647,099; and claims 1-23 were rejected under 35 U.S.C. § 103 over U.S. Patent 5,471,522 (Sells) in view of U.S. Patent No. 5,938,745 (Boyle).

A terminal disclaimer is submitted herewith to obviate the obviousness-type double patenting rejection.

It is respectfully submitted that the Office Action has failed to establish a *prima facie* case of obviousness against the claims over the asserted combination of Sells and Boyle for at least the reason that, even if the references can be combined, the hypothetical combination of Sells and Boyle would not teach or suggest all elements of the claims. *See,* M.P.E.P. § 2143 (8th ed., Rev. 2) at 2100-129.

As conceded by the Office Action, Sells does not disclose the following acts of claim 1: storing permission data relating to security for the system; and determining, based on the permission data relating to security for the system, whether the type of the telephony call is permitted.

The Office Action relied instead upon Boyle as teaching the permission data relating to security for the system as recited in claim 1. Specifically, the Office Action identified the set of identification strings mentioned in Boyle as being the permission data relating to security of the system. According to Boyle, an incoming call received by an arbitrator process is associated with an identification string. Boyle, 2:1-3. Upon receipt of the incoming call, the identification string of the incoming call is compared to the set of identification strings corresponding to applications listening for an incoming call. Boyle, 2:3-6. The set of identification strings that are compared to the identification string of the incoming call correspond to "listening" applications of the port that is being watched by the arbitrator process. Boyle, 4:24-30. If the identification string of the incoming call does not match any identification string of a listening application, the arbitrator process passes the call back as not being for any arbitrated application. Boyle, 4:36-38. However, if a string match occurs, the arbitration process signals the event in the application corresponding to the matching identification string. Boyle, 4:39-43.

The identification strings described in Boyle are merely identifiers of applications that are listening to a port for an incoming call. These identifiers of Boyle cannot be considered permission data relating to security for the system.

Moreover, a further defect of Boyle is that the identification strings are clearly not used to determine whether the *type* of the telephony call is permitted. The identification strings of Boyle are used for matching to an identification string of an incoming call; Boyle provides absolutely no teaching or suggestion that the identification strings can be used to determine whether a *type* of telephony call is permitted.

In view of the foregoing, it is respectfully submitted that the hypothetical combination of Sells and Boyle does not teach or suggest all elements of claim 1. A *prima facie* case of obviousness has thus not been established with respect to claim 1 for at least this reason.

Similarly, with respect to independent claim 13, the asserted combination of Sells and Boyle does not teach or suggest a control element to determine, based on an indication of a type of the telephony call and permission data relating to security for the system, whether the type of the telephony call is permitted. With respect to independent claim 21, the asserted combination of Sells and Boyle does not teach or suggest a microcontroller to determine, based on an indication of a type of telephony call and permission data relating to a target security level, whether the type of telephony call is permitted.

Dependent claims are allowable for at least the same reasons as corresponding independent claims. Moreover, with respect to claim 5, which depends from claim 1, the identification strings of Boyle clearly do not constitute permission data indicating types of telephony calls that are permitted and not permitted based on security requirements of the system. Newly added dependent claims 24 and 25, which depend from independent claims 13 and 21, respectively, are similarly distinguishable over the asserted combination of Sells and Boyle.

With respect to claim 11, which depends indirectly from claim 1, the Office Action stated that because Boyle teaches comparing an incoming string to strings of listening applications, "that one skill [sic] in the art would recognize Boyle in having storage means for storing the set of identification strings, i.e., data relating to security of the system, wherein the set of identification strings are obviously being programmed through a telephony application

programming interface." 8/11/2004 Office Action at 4. There is absolutely no indication that the identification strings of Boyle are set through a telephony application programming interface, as recited in claim 11. The identification strings are merely identifiers of listening applications, and there is no reason to set such identifiers through a telephony application programming interface. No such teaching or suggestion is provided by Boyle or any other reference. Therefore, claim 11 is allowable over the cited references for at least this additional reason.

Dependent claim 12 (which depends from claim 1) recites that the storing, receiving, establishing, detecting, and determining acts are part of a firewall feature. The Office Action stated that "Boyle teaches the arbitrator process for ensuring a given application being worked [sic] with a variety of hardware and configuration (col. 8 lines 53-60) so that one skill [sic] in the art would recognize the storing, receiving, establishing, detecting and determining acting as part of a firewall feature." 8/11/2004 Office Action at 4. The ability of an arbitrator process to ensure that a given application can work with a variety of hardware and configuration does *not* indicate a firewall feature. An ordinary meaning of the term "firewall" is "a system designed to prevent unauthorized access to or from a private network." *See* Webopedia definition of "firewall" (attached). This definition is consistent with the discussion of "firewall" in the specification. *See* Specification, paragraph [005].

The identification strings of Boyle are used to indicate applications that are listening on a particular port. The identification strings are *not* used to prevent unauthorized access to a network. Therefore, claim 12 is allowable for at least this additional reason. Dependent claims 20 and 23, which depend from independent claims 13 and 21, respectively, are further allowable for similar reasons.

In view of the foregoing, allowance of all claims is respectfully requested. The Commissioner is authorized to charge any additional fees and/or credit any overpayment to Deposit Account No. 08-2025 (200304161-2).

Respectfully submitted,

Date: Nov. 11, 2004

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, TX 77024
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

firewall

Last modified: Thursday, August 26, 2004

(fîr´wâl) **(n.)** A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.